



(19)

(11) Publication number: **10240517 A**

Generated Document

PATENT ABSTRACTS OF JAPAN(21) Application number: **09038173**(51) Intl. Cl.: **G06F 9/06**(22) Application date: **21.02.97**

(30) Priority:

(43) Date of application publication: **11.09.98**(71) Applicant: **SONY CORP**(72) Inventor: **WATANABE HIDEKAZU**

(84) Designated contracting states:

(74) Representative:

(54) METHOD AND DEVICE FOR PREVENTING DUPLICATION OF SOFTWARE

(57) Abstract:

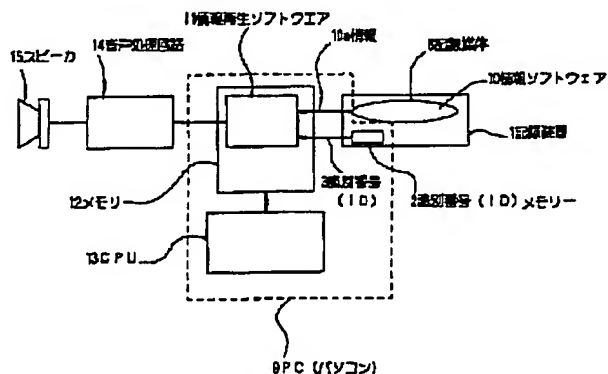
PROBLEM TO BE SOLVED:

To provide a method and a device for preventing the duplication of a software capable of preventing the software loadable to a computer from being easily copied.

SOLUTION:

An identification number(ID) 3 is attached to a recorder 1 capable of preserving the software and the software is provided with a program for inspecting the identification number. At the time of reading the software into the computer 9, the identification number 3 is inspected by the program for inspecting the identification number provided in the software, and when the identification number 3 satisfies inspection conditions, the reproduction of the software is made possible and the duplication of the software is prevented.

COPYRIGHT: (C)1998,JPO

BEST AVAILABLE COPY

(19) 日本國特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平10-240517

(49)公開日 平成10年(1998)9月11日

(51) Int. Cl.⁸
G 0 6 F 9/08

類別號碼
550

F I
G O O F 8/08

550H

審査請求 未請求 請求項の数13 O L (全 10 頁)

(21)出國番号 特願平9-38173

(22) 出願日 平成9年(1997)2月21日

(71) 出票人 000002185

ソニー株式会社

東京都品川区北品川6丁目7番35号

(72) 发明者 渡辺 秀和

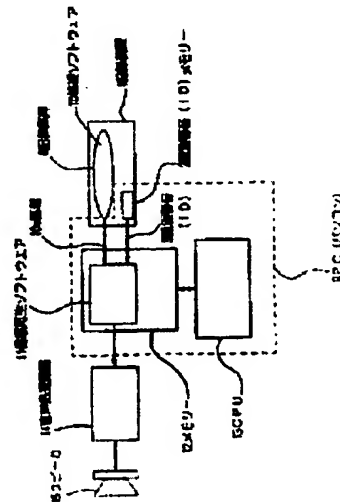
東京都品川区北品川6丁目7番35号 ソニ
ー株式会社内

(54) 【発明の名称】 ソフトウェアの複製防止方法及び装置

(57) 【要約】

【課題】 コンピュータにロードできるソフトウェアを容易にコピーすることを防止できるソフトウェアの複製防止方法及び装置を提供する。

【解決手段】 ソフトウェアを保存することのできる記録装置 1 に、識別番号(1)D3を付し、前記ソフトウェアに前記識別番号の検索用プログラムを含め、前記ソフトウェアをコンピュータ内へ読み出す際、前記ソフトウェアに含んだ前記識別番号の検索用プログラムにより前記識別番号3を検査し、前記識別番号3が検索条件を満たした際、前記ソフトウェアの再生を可能とし、ソフトウェアの複製を防止する。



【特許請求の範囲】

【請求項 1】 ソフトウェアを保存することのできる記録装置に、識別番号を付し、前記ソフトウェアに前記識別番号の検査用プログラムを含め、前記ソフトウェアをコンピュータ内に読み出す際、前記ソフトウェアに含んだ前記識別番号の検査用プログラムにより前記識別番号を検査し、前記識別番号が検査条件を満たした際、前記ソフトウェアの再生を可能としたことを特徴とするソフトウェアの複製防止方法。

【請求項 2】 前記記録装置が記録媒体であることを特徴とする請求項 1 に記載のソフトウェアの複製防止方法。

【請求項 3】 識別番号を付した記録装置と、検査用プログラムを含むソフトウェアとを具備し、前記ソフトウェアをコンピュータ内に読み出す際、前記ソフトウェアに含んだ前記識別番号の検査用プログラムにより前記識別番号を検査し、前記識別番号が検査条件を満たした際、前記ソフトウェアの再生を可能としたことを特徴とするソフトウェアの複製防止装置。

【請求項 4】 前記記録装置が記録媒体であることを特徴とする請求項 3 に記載のソフトウェアの複製防止装置。

【請求項 5】 ソフトウェアにコンピュータに付した識別番号に対応したデータを組み込み、前記コンピュータに前記ソフトウェアを含む識別番号検査用プログラムをロードし、前記ソフトウェアの利用時に、前記識別番号検査用プログラムにより、コンピュータの識別番号と前記ソフトウェアに組み込んだデータとの一致性を検査することを特徴とするソフトウェアの複製防止方法。

【請求項 6】 ソフトウェアに識別番号を用いた暗号化処理を行うステップと、前記暗号化されたソフトウェアを記録装置に保存するステップと、前記ソフトウェアの再生ソフトウェアをコンピュータのメモリに読み出すステップと、前記記録装置又は記録媒体に記憶され暗号化された識別番号を読み出すステップと、前記記録媒体から識別番号から成る暗号を読み出すステップと、前記識別番号の復号化ソフトウェアによって前記暗号と暗号化された識別番号から識別番号を復号化するステップと、前記復号化された識別番号を用いて前記再生ソフトウェアでソフトウェアを再生するステップを含むことを特徴とするソフトウェアの複製防止方法。

【請求項 7】 記録装置に暗号化されたソフトウェアを復号化する復号手段及び識別番号メモリを備え、ソフトウェアの再生ソフトウェアと動作指示プログラムがロードされたコンピュータのメモリを備え、前記識別番号メモリから読み出された識別番号により前記動作指示プログラムにより前記復号手段にコマンドを与え、前記復号手段で前記ソフトウェアを復号化し、前記再生ソフトウェアによりソフトウェアを再生することを特徴とするソフトウェアの複製防止装置。

【請求項 8】 通信ネットワークを通じて、所望のソフトウェアを注文する際、記録装置等に付された識別番号を送信するステップと、受信側では注文された前記ソフトウェアに前記識別番号から付加情報を付加して転送するステップを含むことを特徴とするソフトウェアの複製防止方法。

【請求項 9】 保存されたソフトウェアを利用をする際に、利用者に個別に割り当てられた、利用番号も含めて検査することを特徴とする請求項 1 又は請求項 6 に記載のソフトウェアの複製防止方法。

【請求項 10】 ソフトウェアを保存することのできる記録装置に識別番号を記憶した識別番号記録メモリを備えたことを特徴とする記録装置。

【請求項 11】 ソフトウェアを保存することのできる記録媒体に識別番号を記憶させたことを特徴とする記録媒体。

【請求項 12】 前記ソフトウェアがプログラム、ソフトウェアであることを特徴とする請求項 1 又は請求項 2 又は請求項 5 又は請求項 6 又は請求項 8 又は請求項 9 に記載のソフトウェアの複製防止方法。

【請求項 13】 前記ソフトウェアがプログラム、ソフトウェアであることを特徴とする請求項 3 又は請求項 4 又は請求項 7 に記載のソフトウェアの複製防止装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

【0002】 本発明はパーソナルコンピュータ等にロードするソフトウェアの不正な複製を防止するソフトウェアの複製防止方法及び装置に関する。

【0003】

【従来の技術】 最近ではパソコン通信や、インターネット接続を行っての通信が様々な形で行われており、様々なコンピュータデータやプログラム等のソフトウェアが、デジタルデータとして流通しており、それがハードディスク装置などの記録媒体に最初は代金を支払って合法的に記録された場合でも、その後はダウンロードしたソフトウェアは容易にコピー（複製）可能である。しかも、コピーしたデータはデジタルデータのため、元のものとはまったく同一内容であり、これらを区別することはできない。

【0004】 従って、このようなデジタルデータは、

何回もコピーを取られたり、不正利用されやすかった。PCのプログラムなどのソフトウェアはプログラム自体にプログラムの有効期限を設定することができるので、それを利用してプログラムの長期不正利用を防ぐことができるが、音楽や絵のデータなどの各種デジタルデータはプログラムのように有効期限を付けることも難しく、余り有効な複製防止手段がなかった。

【0005】ここで述べるソフトウェアとしては、PC（パソコン）等で取り扱うことが可能な各種デジタルデータ、音楽データ、画像データなど広範のデジタルデータである。最近のPCは大容量のハードディスク（以下HDDと略す）を備え、そこへ各種ソフトウェアを置き、必要に応じてそれをPC上の処理ソフトウェアを利用し使うことが一般的になっている。

【0006】コピーされたデータはフロッピーディスク（以下FDと略す）や通信回線を通じて他のPCに自由に移動可能であり、これは元のデータを作った者の著作権を無視した不正利用の便道にもなっている。このためソフトウェアの不正利用を防止することは、ソフトウェアを配布する上では、大きな課題となっている。

【0007】特に近年では、インターネットや、パソコン通信などのコンピュータネットワークを通じて、ソフトウェアを配布することが一般的に行われるようになってきているので、そのようなソフトウェアの不正利用を防止することは急務になってきている。このようなソフトウェアの場合、利用者がソフトウェアを購入するにも店舗に行く必要はなく、ネットワークを通じて必要なものを入手できるため、大変便利であるが、一方ソフトウェアを販売する側としては、PCなどで簡単に複製可能なデジタルデータをネットワークで伝送することは、データの不正コピーが作りやすいという点で、大きな問題となる。

【0008】又はこれとは別に、記録メディアの進歩により、従来より使われていたHDD、FD、磁気テープなどとは別にMO、PD、ZIP、媒体交換可能型HDD、OptoMOなど多くの種類の大容量記録媒体が開発され、しかもこれらのものは記録媒体のみを携帯して持ち運ぶことも可能である。これらの記録媒体を使用すれば、異なるPC間でデータをコピーし交換することも容易である。従って、これも又はソフトウェアの不正利用の点では、問題である。

【0009】しかしコンピュータのユーザーにとっては、これらの記録媒体を使用することで簡単にソフトウェアを持ち運んだり、バックアップを取ったりすることができるため、これらの使用を禁止することは現実的ではない。従って、このような記録媒体を今迄どおりに使用しながら、ソフトウェアの不正利用を防止する技術が強く求められている。

【0010】本発明はそのような技術の一つであり、記録媒体又は記録装置に、利用者からは複製困難なユニ

ークな番号を書き込んでおくことにより、ソフトウェアの不正使用を防ぐためのものである。

【0011】これらの記録装置は図11に示すように、ディスクトップ型のPC（パーソナルコンピュータ）9の場合にはSCSIと呼ばれる周辺機器インターフェースを利用してPC9と記録装置1が接続されることが多い。そしてFD、MO、PDといった記録媒体8は、それを動作させるための機構（ドライブ）と記録媒体8そのもの（メディア）を分離することができ、必要ときに必要な記録媒体8をそれを使うための機構に挿入することで、自由にソフトウェアの読み出し、書き込みができるようになっている。

【0012】又は、SCSIを用いて外付のHDDを接続することも可能である。このようなHDDの場合、通常は記録媒体8を記録装置から分離することはできない。又はノート型PCなどの携帯型端末では、図12に示すごとく、端末のインターフェースとしてPCMCIAインターフェースと呼ばれるものを持ち、これを使用して外部機器とPC9を接続できるようになったものが、最近は多くなっている。PCMCIAインターフェースはカード型のインターフェースカードをPC9本体に挿入して使うことができ、小型機器のインターフェースとしては使いやすいものである。

【0013】PCMCIAインターフェースカードは、もともとメモリーカードが出发点であり、メモリーカードとして様々なデータを記憶できるものもあるが、現在ではメモリーカードだけではなく様々な種類のものがあり、上述のSCSIインターフェース用のカードなどもある。SCSIインターフェース用のPCMCIAカードを使用したときには、SCSIを利用し、PC9と外部装置を接続することも可能である。

【0014】又は、PCMCIAカードの中にはそれ自体がハードディスク装置になっているものもあり、その場合には図12に示すように、PCMCIAカード型HDD装置（記録装置1）をPC9に接続するだけで、データの読み書きができるようになる。従って、この場合にはPCMCIA型HDD装置自体を、FDのように自由に持ち運んで使用することもできる。

【0015】本発明はこのような記録媒体を用いて、音楽データや画像データといったソフトウェアを利用するときにその不正利用を防止するためのものである。このような記録媒体にあるソフトウェアを記憶して利用するとき、上述のようにPCでは通常簡単にデータファイルのコピーができるので、記録されたソフトウェアを不正にコピーしそれをPC内部のHDDに移して利用するようなことは難しくない。

【0016】それを防止するために、本発明では記録媒体又は記録装置にユニークなナンバーから成る識別番号（ID）を付け、そのIDを利用し、HDDに記録するソフトウェアの検査を行い、不正コピーの防止を行うもの

である。10は記録媒体に記録しても良いし、それを操作するための記録装置本体に記憶しても良い。通常のHDDの様に記録媒体と記録装置が一体化されたものももちろん10が書き込まれていても問題はないが、記録装置にハードウェア的に書き込まれていたほうが、10を簡単に書き換えできず安全性の点で扱いやすい。

【0017】

【発明が解決しようとする課題】本発明はコンピュータにロードできるソフトウェアをコピーすることを防止できるソフトウェアの複製防止方法及び装置を提供することを目的とする。

【0018】

【課題を解決するための手段】請求項1に係る本発明のソフトウェアの複製防止方法は、ソフトウェアを保存することのできる記録装置に、識別番号(10)を付し、前記ソフトウェアに前記識別番号の検査用プログラムを含め、前記ソフトウェアをコンピュータ内に読み出す際、前記ソフトウェアに含んだ前記識別番号の検査用プログラムにより前記識別番号を検査し、前記識別番号が検査条件を満たした際、前記ソフトウェアの再生を可能とし、ソフトウェアの複製を防止する。

【0019】請求項3に係る本発明のソフトウェアの複製防止装置は、識別番号を付した記録装置と、検査用プログラムを含むソフトウェアとを具備し、前記ソフトウェアをコンピュータ内に読み出す際、前記ソフトウェアに含んだ前記識別番号の検査用プログラムにより前記識別番号を検査し、前記識別番号が検査条件を満たした際、前記ソフトウェアの再生を可能とし、ソフトウェアの複製を防止する。

【0020】請求項5に係るソフトウェアの複製防止方法は、ソフトウェアにコンピュータに付した識別番号に対応したデータを組み込み、前記コンピュータに前記ソフトウェアを含む識別番号検査用プログラムをロードし、前記ソフトウェアの利用時に、前記識別番号検査用プログラムにより、コンピュータの識別番号と前記ソフトウェアに組み込んだデータとの一致性を検査し、ソフトウェアの複製を防止する。

【0021】請求項6に係る本発明のソフトウェアの複製防止方法は、ソフトウェアに識別番号を用いた暗号化処理を行うステップと、前記暗号化されたソフトウェアを記録装置に保存するステップと、前記ソフトウェアの再生ソフトウェアをコンピュータのメモリに読み出すステップと、前記記録装置又は記録媒体に記録された暗号化された識別番号を読み出すステップと、前記記録媒体から識別番号から成る暗号番号を読み出すステップと、前記識別番号の復号化ソフトウェアによって前記暗号番号と暗号化された識別番号から識別番号を復号化するステップと、前記復号化された識別番号を用いて前記再生ソフトウェアでソフトウェアを再生するステップを含むソフトウェアの複製を防止する。

【0022】請求項7に係るソフトウェアの複製防止装置は、記録装置に暗号化されたソフトウェアを復号化する復号手段(復号用ハードウェア)及び識別番号記録メモリ(10メモリ)を備え、ソフトウェアの再生ソフトウェアと動作指示プログラムがロードされたコンピュータのメモリを備え、前記識別番号記録メモリから読み出された識別番号により前記動作指示プログラムにより前記復号手段にコマンドを与え、前記復号手段で前記ソフトウェアを復号化し、前記再生ソフトウェアによりソフトウェアを再生し、ソフトウェアの複製を防止する。

【0023】請求項10に係る記録装置はソフトウェアを保存することのできる記録装置に識別番号を記録した識別番号記録メモリ(10メモリ)を備えた構成とし、ソフトウェアの複製を防止する。

【0024】

【発明の実施の形態】以下に本発明の好適な実施の形態について、図面を参照しつつ詳細に説明する。

第1の実施の形態

このような識別番号(10)は利用者によって簡単に書き換えられないように、設定されている必要があり、図1に示すように記録装置1内部のROM2(Read Only Memory)などに識別番号(10)3がハードウェア的に書き込まれていれば、書き換えに対する安全性は高い。

【0025】記録装置1は例えばハードディスク駆動装置であり、制御回路4にROM2、書き込み回路5、読み出し回路6、1/F(インターフェース)回路7を接続し、図示しない機構部にセットされた記録媒体(例えばハードディスク)8にデータを書き込んだり、読み出す。又は、図示しないパソコン9との間で、これらのデータを1/F7を介してやりとりする構成となっている。

【0026】第2の実施の形態

記録媒体に10が書き込まれる場合にも、通常は利用者によって書き換えることのできない記録媒体の領域、例えば図2に示すように記録媒体(ハードディスク)8全体の状態を制御するための領域(管理データ領域9a)や、通常では使うことのない記録媒体上のデータ領域間の隙間などに識別番号(10)9を書き込むことにし、一般の利用者は109を簡単に書き換えることができないようにしておく。

【0027】尚、管理データ領域9aはセクター9aで区切られた領域に設けられている。このようなしておかないと不正利用者に10を書き換えられソフトウェアの不正コピーをされてしまう虞もある。以下に、このような10を用いて、どのようにソフトウェアの不正利用を防ぐのが説明する。ここでは記録媒体としてハードディスク(HDD)、記録装置としてハードディスク駆動装置を想定して説明を行うが、他の記録媒体と駆動装置でも、まったく同様である。

【0028】第3の実施の形態

この第1の方法は、記録されているデジタルデータの使用時に、記録装置又は記録媒体に書かれているIDを直接チェックすることで、不正利用防止を行う方法である。図3は音楽が記録されたデータ（情報ソフトウェア10）を、PC（パソコン）9を用い音楽を聴くための機能ブロック図であり、PC9に記録装置1の記録媒体8から音楽等の情報10を供給し、又は再生に当たりメモリー12に置いた情報再生ソフトウェア11を用いて音楽を再生する。

【0029】情報再生ソフトウェア11にて再生される音楽情報はD/A変換器、増幅器等を含む音声処理回路14からスピーカ15に至り、音声として出力される。これらの処理はCPU13の制御の下に実行される。そして、この場合は記録装置1にROMからなる識別番号（ID）メモリー2が備えられ、IDメモリー2には記録装置1側に個別のID3が付されている。情報再生ソフトウェア11はプラグイン式のもので一般的であり、通信手段やCD-ROM等から、ハードディスク等の記録媒体8にロードされる。

【0030】そして、音楽再生のための情報再生ソフトウェア11にIDチェックのためのプログラムを予め組み込んでおき、再生時に、このプログラムを用いてIDメモリー2に含まれたID3をチェックし、それが正しいものであるれば再生を実行し、IDが不当な場合には再生を実行しないようにして、ソフトウェアの不正利用防止を図る。

【0031】尚、この場合はID3を記録装置1に設けたIDメモリー2に付したが、内蔵ハードディスク等の記録媒体8の管理領域に付しても同等である。又は、IDのチェックに際しては、再生するソフトウェアにチェックを要することを表す符号が書かれているときにのみ、それを行うようにしても良い。そのようにしておけば、自由に配布可能なソフトウェアの場合には、識別番号無しで配布すれば、利用者は自由にコピーしてそれを使うことが可能になる。

【0032】このようなIDにより、データの不正利用防止が可能になるが、IDが書かれていないことは、すぐに認識できるものの、情報ソフトウェア10に不正にIDが書き込まれている場合のことも考慮し、IDは適当に振られるのではなく、ある規則に従って作成されるほうが良い。例えば、IDが10桁程度の整数からなるものとする、下5桁と上5桁に分けて考え、上5桁の数Yは下5桁Xの数からある規則（関数f）によって生成されるようにしておく。

【0033】 $Y = f(X)$

例えば簡単にXに123（適当な数）を掛け、その下5桁をYとするような方法であっても良い。関数が複雑なものであれば、それだけIDは不正に類推、生成しにくくなる。こうしておけば、IDの生成規則を知らない

限り、任意の数もIDとしてHDに書き込み、音楽データなどを不正使用することはできなくなる。再生を行うソフトウェアはこの生成規則からIDの正当性をチェックすることが可能である。

【0034】尚、このような方式の場合、音楽再生用プログラムのようなデータを扱うためのソフトウェアは、ソフトウェアの利用を会員制等の形で、予め登録された会員にのみ配布しておく必要がある。このような会員には通常、会員番号が考えられることが多いので、この会員番号を利用してソフトウェアの不正利用を防止することも可能である。

【0035】しかし上述の方法では、正当なIDが書き込まれたHD同士でソフトウェアがコピーされた場合には、チェック用のプログラムを有した情報再生ソフトウェアでもIDのチェックは通過するため、ソフトウェアの不正利用が防げないという問題がある。これを防ぐために、以下に述べるような第2の方法がある。

【0036】第4の実施の形態

そこで、HDに記録されたソフトウェアにも、IDに対応した何らかのデータを付加し、不正利用を防ぐ方法である。従ってIDに対応してソフトウェアの内容も一部書き足すことになるので、この方法では現在のようにCD-ROMのような形で同じ内容のものを利用者に配布することはできなくなり、利用者の持つHDのID毎にソフトウェアの内容を書き換える必要がある。

【0037】しかし現在では、コンピュータネットワークを通じてデータをやりとりすることも可能になっているので、このような場合には、ここで述べるような方法で、ユーザーからソフトウェアの購入注文があった場合、そのユーザーの持つIDに従って、ソフトウェアを書き換え、それを利用者に送ることもさほど困難性はない。このような処理はコンピュータ通信により行うことが可能である。

【0038】第5の実施の形態

具体的な例として図4にネットワークによるソフトウェアの発注、転送システムの概念図を示して説明する。コンピュータネットワーク16は今日陸盛なインターネットであり、利用者17はパソコン9を利用してサービスセンター18に必要とするソフトウェアを注文する。その際ハードディスク（記録媒体）8に付されたIDを連絡する。

【0039】そして、サービスセンター18では注文に応じた情報をデータベース19から取り出し、連絡されたIDからソフトウェアデータへの付加情報を生成し、付加する。そしてそのソフトウェアを利用者17に転送する。

【0040】尚、ここでは利用者17がIDをコンピュータネットワーク16を通じてサービスセンター18に送るようになっているが、サービスセンター18では利用者17のもつHD8のIDを予め登録しておけば、利用

者17が注文時にIDをサービスセンターに送る必要は省略できる。

【0041】PC上の音楽再生ソフトウェアでは、HDD自体のIDとソフトウェアに書かれている暗号（以降S1Dと略す）を比較し、S1DとIDの対応が取れれば記録されたデータを再生するようにする。対応が取れなければ、データの再生を行わない。このようなしておけば、HDD上のソフトウェアはそのHDDがない限り再生ができず、ソフトウェアの不正利用防止ができる。

【0042】S1DとIDの対応は、どのようなものでも良く、まったく同じのものであっても構わないが、同じであるとは何かの手段で不正利用がされやすくなるので、検測されにくくする方法として、例えば次のようなIDの構成法がある。即ち、適当な関数 $f()$ 、 $g()$ を使い、次のような関係で生成できるようにする。

【0043】 $S1D = f(ID)$ 又は $ID = g(S1D)$

関数 $f()$ 又は $g()$ は図4で示すサービスセンター及びPC側のデータ再生用ソフトウェアでは、どのような規則のものかわかっている必要があるのは無論のことである。そうでないと、サービスセンターでIDに対応したS1Dが生成できないし、再生用ソフトウェアではS1DとIDの対応関係がわからないため、データの不正利用をチェックできない。

【0044】上述のような方法でも、データ自体はそのままの形であるので、適当な方法でS1Dの含まれていないデータを抜き出し、それをコピーして不正利用されることも考えられる。

【0045】第6の実施の形態
これを防ぐために、記録されるデジタルデータを符号化（暗号化）しておき、それを読み出すときに復号化し元のデータを取り出すようにする。ここでこの方法を簡易に説明するために、デジタルデータの暗号化方法について説明をする。

【0046】暗号化は元の内容がわからないようにデータを変換する技術であり、具体的には元のデータを鍵データを使った関数（暗号アルゴリズム）で暗号データに変換するものである。図5に示すように、デジタルデータの暗号化方法については2種類に分けることができる。

【0047】図5（a）に示す共通暗号化方式は暗号化、復号化の過程で同じ鍵データK（キーワード）を使うものであり、鍵データKは通常秘密にする必要がある。図5（b）に示す公開暗号化方式は暗号化と復号化のときの鍵データに異なるものを使用するもので、この場合2つの鍵データ K_e 、 K_d の内一つは公開されていても、暗号安全性の面では問題はないとされており、復号操作は複雑なものの方の鍵が個人的に秘密にされるため、本人認証や、データの正当性を保持するためにこれが使われることも多くなってきている。

【0048】以上の暗号化方式を元に、ここでは暗号化鍵としてIDやS1Dを使って、データの不正利用を防止することを提案する。データの暗号化鍵としてID又はS1Dを利用すれば、データを暗号化して伝送することができる。

【0049】第7の実施の形態

図5（a）は本発明の共通暗号化方式を利用した転送方式の概念図であり、図5（b）は公開暗号化方式を利用した転送方式の概念図である。

【0050】通常IDはHDDから読み出し可能であるので、利用者にIDがわかってしまうという意味では共通暗号化でも公開暗号化でもどちらでも、データのセキュリティ上は問題がある。特に公開暗号化はデータの正当性を利用者側でチェックする必要がある場合以外は、復号作業が複雑化しやすいので、この方法を使用する必要性は少ない。

【0051】IDが読めるとしても通常はデータが暗号化されていれば、利用者が簡単にデータの内容を読めるわけではないので、データの不正利用防止の効果はある。共通暗号化でも、高麗な安全性が求められる場合は別であるが、通常は鍵データがわかって、暗号アルゴリズムが公開されていなければ、簡単に元のデータが得られるわけではないので、IDを鍵として使っても余り問題はない。又は、IDは利用者が直接使う必要はないので、簡単な手段では利用者がIDを読み出せないようにできれば、データの不正利用の安全性はさらに高まる。

【0052】IDを読みにくくする手段としては、ID読み出しの手順を複雑化し、HDD装置に対する単純なコマンド一つだけでは、IDが読み出されないようにしておけば、利用者がIDを読み出すのは困難となる。この場合でも記録されたソフトウェアを利用するためのPC上のソフトウェア（プログラム）では、予めその手順をプログラムしておけば、それによりIDを読み出すことができるので、実際のデータの読み出しには何ら問題はない。

【0053】IDを利用者が利用しにくくする手段として、ID自体を予め暗号化しておくことも有効である。IDを暗号化してHDDに記録しておけば、それを適当に変換することも難しくなり、これもソフトウェアの不正利用防止には効果がある。但しこの場合、利用者が持つIDは予めサービスセンターで把握しておく必要がある。暗号化されたIDは、サービスセンターからソフトウェアに付随して送られる暗号鍵IDKで、復号化されるようにする。

【0054】第8の実施の形態

図7にこの方法を利用したソフトウェアの暗号化、図8に復号化の過程を示す。即ち、サービスセンター側では、暗号化データ20aにデータSを供給して鍵データS1Dによって暗号化し、このデータにIDK付加す

コード21を付加し、暗号文データcs1dとして利用者のパソコン9に供給する。そしてパソコン9に付属されたハードディスク駆動装置(記録装置1)のHDBに暗号文データcs1dを記録する。

【0055】暗号データの復号化は図8に示すごとく、暗号文データから成る音楽ソフトウェア22をHDBから読み出し、音楽再生ソフトウェア23に供給する。同時に音楽ソフトウェア23に含む暗号データIDKを読み出し、IDの復号化ソフトウェア24に供給する。

【0056】一方記録装置1からは暗号化されたID3が読み出され、IDの復号化ソフトウェア24に供給される。IDの復号化ソフトウェア24では暗号データIDKにより、暗号化IDの復号化が行われる。そして復号化されたID3を用いて音楽再生が復号化処理を含んで実行される。

【0057】尚、この図8ではIDによるデータの復号化をPC上のソフトウェアで行っているが、前述のようにハードウェアで行うことも考えられる。尚、図8のデータの復号化では図3に示した再生方式と対比し音楽データの復号化の例を示しているが、画像データやテキストデータの復号化でも再生手順は同じであり、データの出力先がスピーカからディスプレイに変わるだけである。

【0058】上記説明では暗号化されたデータの復号化は、PC上のCPUでソフトウェアによって行われるものとして説明を行ったが、暗号化、復号化処理はその処理アルゴリズムによっては多大な計算量を必要とするものもあるため、復号化専用ハードウェアでその処理を行うことも良い。

【0059】第9の実施の形態

ここではデータの復号処理に用いる復号用ハードウェア25は、記録装置1に内蔵した形でもPC9上に備えられた形でも構わない。

【0060】暗号化された音楽データを再生する場合の処理システムブロックを図9に示す。この例では、暗号化されたデータである音楽ソフトウェア22を復号化するとき、まずPC9上にロードされた音楽再生ソフトウェア11で記録装置1のID3を認識し、それが正確なものであるれば、記録装置1の復号用ハードウェア25に対し、それが動作するよう適当なコマンド26を出力する。

【0061】その後暗号化されたデータを復号用ハードウェア25を用いて復号化し、それをPC9に転送しPCでデータ再生を行う。HDB上の暗号化されていないデータIDbを利用する場合には、図9の点線矢印で示すように復号用ハードウェア25を bypass してPC9にデータIDbを転送する。以上のようにすれば、PC9に復号化処理ソフトウェアを持つ必要はないので、複雑な復号化処理が必要な場合でもCPUに余分な負荷がかかることを避けることができ、CPUに不必要に高性能なものを使う必要もなくなる。

【0062】請求項9で述べた、利用者番号(以下UIDと略す)の利用はデータ再生ソフトウェアでHDB上のデータを再生するときに、IDやSIDなどの番号の他に利用者番号など別の番号をソフトウェア再生のための認証に利用するものである。前述のようにオンラインで有料データを転送する場合には、利用者番号等をサービスセンターに登録するのが普通であり、サービスセンターではこれを利用者名簿などに登録しておく。

【0063】従って、これをIDと共に利用してソフトウェアの不正利用防止を行うことが可能である。IDを利用しないでUIDだけをIDのように利用してソフトウェアの不正防止をすることも可能であるが(実際これは既に行われている方法である)、IDと共に使うことで、データのセキュリティを高めることが可能である。

【0064】UIDはデータ再生ソフトウェアを利用するたびに利用者が入力する方法でも良いが、予めUIDを別のファイルに書き込んでおき、それをデータ再生ソフトウェアが読んで利用する方法もある。若干利用者にとっては面倒ではあるが、ソフトウェアを使用するときUIDを入力する方法がデータ保護の点では望ましいだろう。又は、サービスセンターがデータ再生ソフトウェアを利用者に提供するとき、そのソフトウェアにUIDを組み込んでおく方法も考えられる。

【0065】UIDはIDと同様に利用することが可能であり、例えば図10のようにUIDとIDを組み合わせて一つの新しいIDとして利用し、データの正当性をチェックしたり、又は同様にSIDと組み合わせたりして、データチェックのために利用することが可能である。IDと組み合わせるとUIDをSIDと同様に使えば、CD・ROMのような大量に同じ内容のものを配布する場合(この場合SIDが使えない)、データの不正利用防止の効率は高い。

【0066】又は、請求項1から請求項9で述べた方法を組み合わせれば、データの不正利用を防ぐことも有効である。例えば、ID、SID、UIDといった識別番号を組み合わせれば、それをお互いに利用してデータのチェックを行ったり、復号化処理を行ったりすることは様々な組み合わせ方法が考えられ、それによりデータの不正利用防止を一層強化することができる。

【0067】以上の説明は、PCなどのコンピュータで一般的に使われているHD(ハードディスク)を例に行ったが、このようなデータの保護機構は他の記録装置、例えば磁気テープ記録装置やMOなどの光磁気記録装置などにも幅広く利用できる。

【0068】又は記録装置に記録するソフトウェアとしても本文では音楽を演奏するためのデジタルデータを例にとって説明を行ったが、本発明で保護対象となるソフトウェアはこれに限らず、記録装置に記憶可能なデジタルデータであれば、画像データであって文書データであっても、コンピュータのプログラムであっても、同

様な手法で、ソフトウェアの不正使用防止を行うことができる。

【0069】さらに、以上の説明はコンピュータの利用を前提として行ったが、このような記録装置の記録内容の保護方式は、例えばデジタル記録方式の音楽再生専用機の様な明示的にコンピュータを使ってはいない装置にも適用でき、一般的な記録保護方式として利用することも可能である。

【0070】
【発明の効果】本発明を用いることにより、ハードディスク装置などの記録媒体に記録されたソフトウェアのコピーが増しくなり、不正コピーを防止できる。特にネットワークなどを通じて、ソフトウェアを配送する場合でもそれを利用できるのは機器の識別番号が特定できるものだけであり、ネットワーク上で配送途中のデータが盗まれたり、利用者によってコピーされても他のPCなどではそれを利用することができず、不正利用を未然に防止できる。その結果、各種ソフトウェアを提供する企業もネットワークなどを通じてソフトウェアを安心して利用者に配信可能になる。

【図面の簡単な説明】

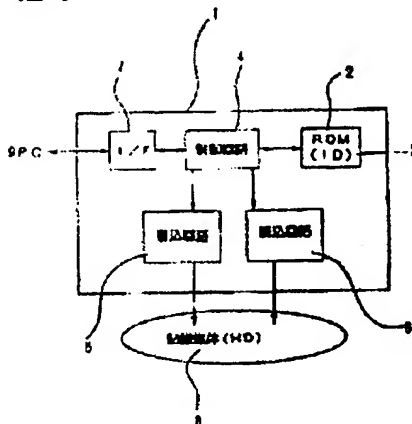
【図1】 本発明のIDメモリーを備えた記録装置の回路ブロック図。

【図2】 本発明のIDを付した記録媒体の平面図。

【図3】 本発明のパーソナルコンピュータによる音楽再生システムブロック図。

【図4】 ネットワークによるソフトウェアの発注、経送システム概念図。

【図1】



【図5】 暗号化方式のシステム概念図。

【図6】 本発明の暗号法を利用した経送方式。

【図7】 本発明のIDKを付加した暗号データの経送方式概念図。

【図8】 音楽データを再生するためのIDの暗号化と復号化システムの概念図。

【図9】 本発明のハードウェアによるIDの復号化方式の機能ブロック図。

【図10】 UIDとIDの組み合わせ原理図。

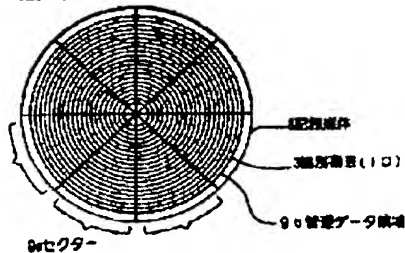
【図11】 各種記録媒体とデスクトップ型PCの接続を示す機能概念図。

【図12】 ノート型PCとPCMCIA型HDの接続を示す機能概念図。

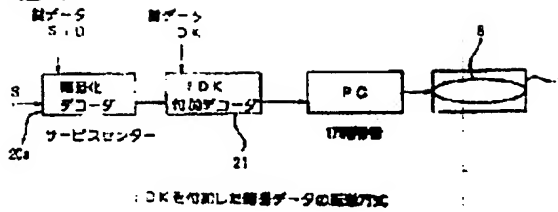
【符号の説明】

1…記録装置、2…識別番号(ID)メモリー、3…識別番号(ID)、4…制御回路、5…書込回路、6…読込回路、7…I/F、8…記録媒体、9…パソコン、9a…セクター、9b…管理データ領域、10…情報ソフトウェア、11…情報(音楽)再生ソフトウェア、12…メモリー、13…CPU、14…音声処理回路、15…スピーカ、16…コンピュータネットワーク、17…利用者、18…サービスセンター、19…データベース、20…暗号データ、20a…暗号化デコーダ、21…IDK付加デコーダ、22…音楽ソフトウェア、23…音楽再生ソフトウェア、24…IDの復号化ソフトウェア、25…復号用ハードウェア、26…動作指示プログラム、26a…コマンド

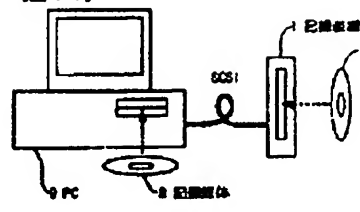
【図2】



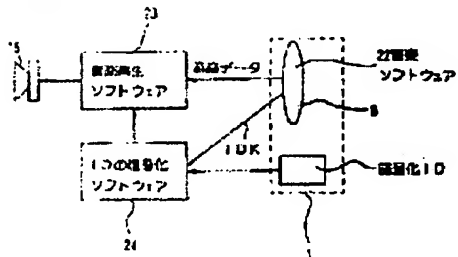
【図 7】



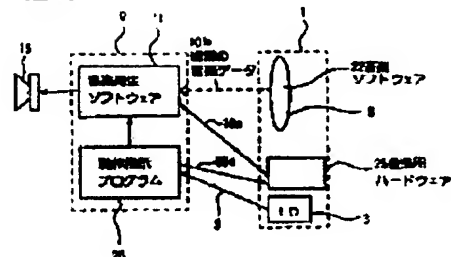
【図 11】



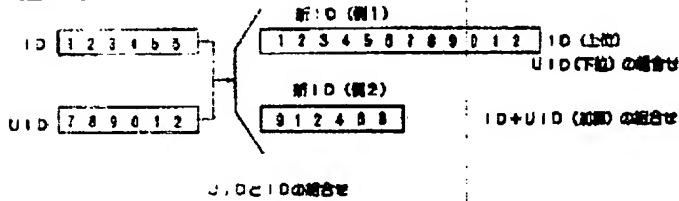
【図 8】



【図 9】



【図 10】



**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☒ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.